Datentransfer & Cloud Computing

Christopher Götz, LL.M. (New York)

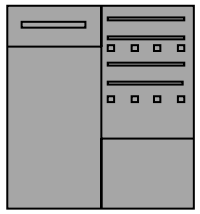
BVMed Akademie - Online Seminar
1. Oktober 2025

§

Cloud Computing & Datentransfers

Moderne u. leistungsfähige IT-Systeme zur Datenverarbeitung erforderlich

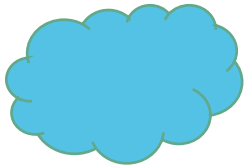
Aufbau eigener IT-Infrastruktur



Beauftragung externer Unternehmen mit

- Aufbau der IT-Infrastruktur
- evtl. Softwareerstellung
- Wartung der IT-Systeme
- regelmäßigen Upgrades

Rückgriff auf Systeme Dritter



Cloud Computing (Daten-Hosting durch Service Provider)

- Anbindung an Internet genügt
- Keine Wartung erforderlich
- Updates/Upgrades werden automatisch vorgenommen

Cloud Computing

Anwendungsbeispiele

- Nutzung von Speicherplatz „in der Cloud“ (Drittserver in Rechenzentrum)
- Nutzung von MS Office 365 (keine Installation, Browser genügt)
- Nutzung von sonstigen Software-as-a-Service-Tools bezogen auf HR-, CR- oder Reisemanagement (z.B. Salesforce, Workday, Concur)
- AI-as-a-Service

➢ Digitalisierung von Unternehmen:

  ➢ Sprunghafte Zunahme

Problem?

➢ Datenübermittlung von personenbezogenen Daten an Service Provider, z.B.

- Mitarbeiterdaten (z.B. Basisdaten, Krankheitstage)
- Daten von Geschäftspartnern (z.B. Ärzte, Lieferanten)
- Patientendaten (z.B. Kontaktdaten, sensible Daten)
- „Sozialdaten“ (pers.bez. Daten, die von einem Leistungsträger, insbes. Gesetzl. Krankenkassen im Hinblick auf ihre Aufgaben nach dem SGB X verarbeitet werden → § 67 Abs. 2 SGB X)

➢ Zum Teil Übermittlung in Länder ausserhalb der EU

- „Schrems II“

Fragen

§

- „Verbot mit Erlaubnisvorbehalt“ – gilt dieser DSGVO - Grundsatz auch für eine Datenübermittlung?
- Bei Konzernunternehmen: Gibt es ein Konzernprivileg?
- Welche Relevanz hat die Auftragsdatenverarbeitung?
- Gelten Besonderheiten bei Patientendaten?
- Gelten Besonderheiten bei Datenübermittlungen in einen Drittstaat?

„Verbot mit Erlaubnisvorbehalt“

§

- Datenschutzrechtlicher Grundsatz (Art. 6 Abs.1 lit a – f EU-DSGVO):

„*Verarbeitung*“ von *personenbezogenen* Daten einer *natürlichen* Person

(Betroffene) ist **nur rechtmäßig, soweit**

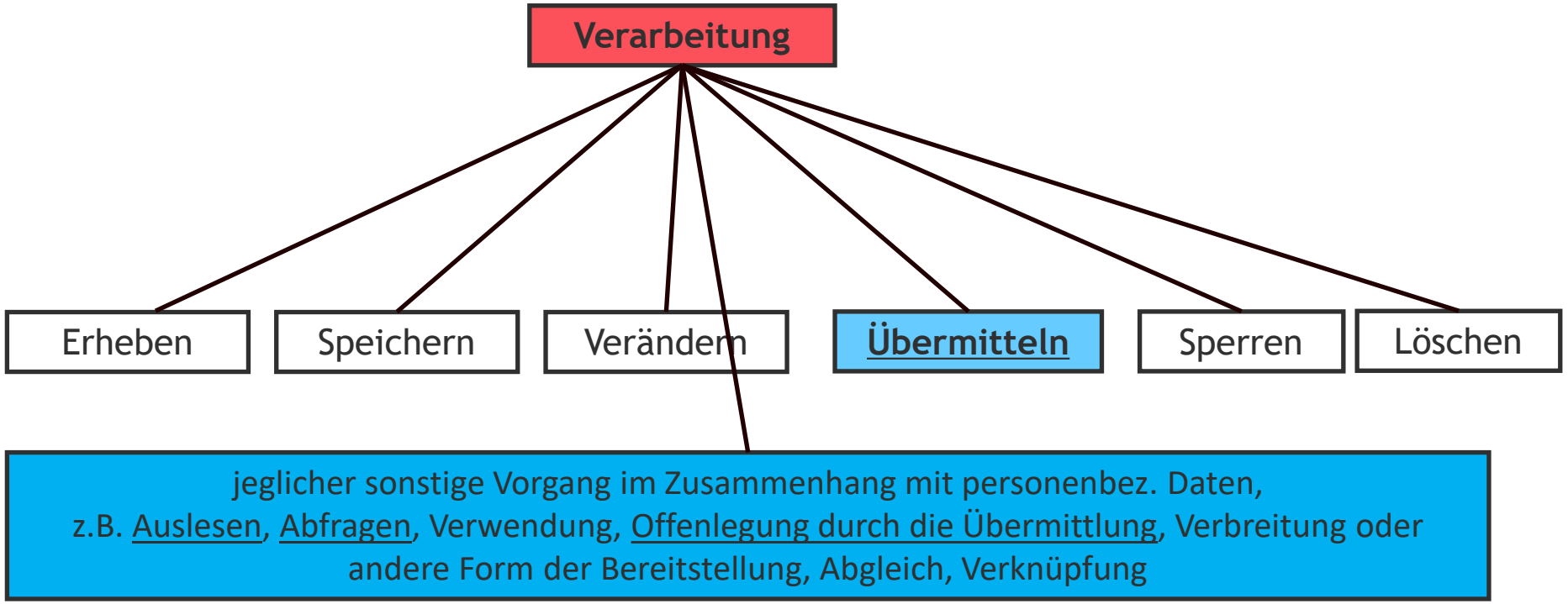
- Einwilligung **des Betroffenen oder**
- Erlaubnistatbestand

vorliegt.

§

„Verarbeitung“

- **„Verarbeitung“ = Datenübermittlung?**
- Definition Artikel 4 Nr. 2 DSGVO:



§

Rechtmäßigkeit der Datenübermittlung

❑ **Konsequenz:**

Datenübermittlung **nur rechtmäßig, soweit**

- **Einwilligung des Betroffenen oder**
- **Erlaubnistatbestand vorliegt**

➢ Bei Verstoß drohen **Sanktionen von bis zu 4% des weltweiten Jahresumsatzes oder EUR 20 Millionen**

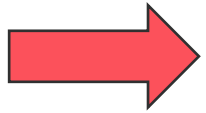
Rechtmäßigkeit der Datenübermittlung

§

Problem: **Feststellung eines Erlaubnistatbestands regelmäßig kompliziert bzw. mit Güterabwägung verbunden;**

Einholen einer Einwilligung häufig nicht praktikabel & mit Risiken verbunden!

Frage: **Ausnahmen zu vorgenanntem Erlaubnisvorbehalt?**



Auftragsdatenverarbeitung, Art. 28 DSGVO?

§

Auftragsdatenverarbeitung

❑ **Privilegierung** der Auftragsverarbeitung iSd Art. 28 DSGVO!

- Datentransfer (von Auftraggeber zu Auftragnehmer bedarf weder eines Erlaubnistatbestands noch einer Einwilligung!
- Verarbeitung bzw. Nutzung der übermittelten Daten durch den Auftragnehmer bedarf ebenso wenig einer Rechtfertigung!

➢ Achtung: Daten müssen selbstverständlich von der Verantwortlichen Stelle rechtmäßig erhoben worden sein und von ihr grds. verarbeitet werden dürfen)

„Auftragsverarbeitung“, Art. 28 DSGVO

§

- **Voraussetzung** einer rechtmäßigen Auftragsvereinbarung:
  - **Weisungsgebundenheit (**Erw. 81, Art. 28, Art 29)
    - Auftragnehmer = "verlängerter Arm" des Auftraggebers
    - vollständig weisungsgebunden!
    - kein eigenes Ermessen!

    Achtung: sofern keine Weisungsgebundenheit → Datentransfer zwischen zwei Verantwortlichen Stellen („Funktionsübertragung“) (keine Privilegierung des Datentransfers!)

  - **Auftragsverarbeitungsvertrag**
    - **Mindestinhalt:** Art. 28 Abs. 1, 2 und 3 lit. a - h DSGVO

Auftragsverarbeitungsvertrag – Mindestinhalt (Art. 28 DSGVO)

§

- Gegenstand und Dauer des Auftrags
- Umfang, Art, Zweck d. Verarbeitung/**Art der Daten/Betroffenenkreis**
- **Technische und organisatorische Sicherheitsmaßnahmen**
- **Berechtigung zur Unterbeauftragung**
- Weisungsgebundenheit & Verschwiegenheit
- **Unterstützung des Verantwortlichen** in Bezug auf
  - Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte & Einhaltung der TOMs,
  - **Meldepflichten ggüber Behörden und Betroffenen (Art. 33, 34),**
  - **Datenschutzfolgeabschätzung (35, 36)**
- Kontrollrechte des Auftraggebers (**Audit Recht**) sowie Duldungs- und Mitwirkungspflichten des Auftraggebers
- Mitteilungspflichten bei Verstößen
- Rückgabe/Löschung von Daten nach Auftragsbeendigung

Auftragsverarbeitungsvertrag – Standardverträge?

§

❑ Art. 28 DSGVO - Standardvertragsklauseln der EU Kommission vom 4. Juni 2021

- Erlaubt, *diese „in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Standardvertragsklauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.“*

§

Besonderheit: Patientendaten (I)

❑ Problem: § 203 StGB - Verletzung von Privatgeheimnissen?

- **Einschaltung von „Auftragsdatenverarbeitern“ zulässig?**

„Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm (u.a.) als Arzt, Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“

- **November 2017: Gesetz zur** Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen
- **Konsequenz: Verwendung von Cloud Computing Lösungen Dritter damit grds. zulässig** (Abs. 3 HS 2 – „sonstige Mitwirkende“)!
- **Aber Achtung:**
  - Service Provider muss auf Geheimhaltung verpflichtet werden (Abs. 4 Satz 2 Nr. 1)
  - Service Provider muss seine Mitarbeiter auf Geheimhaltung verpflichten (Abs. 4 S. 2 Nr. 2)

Neu seit 1. Juli 2024: § 393 SGB V

§

1) **Leistungserbringer** im Sinne des Vierten Kapitels (*Erbringen Leistungen für die Versicherten der Krankenkassen, u.a. Vertragsärzte, Krankenhäuser, Apotheken*) und Kranken- und Pflegekassen sowie ihre jeweiligen **Auftragsdatenverarbeiter** dürfen **Sozialdaten und Gesundheitsdaten** auch im Wege des **Cloud-Computing**-Dienstes (→ *Def. § 384 Nr.5 SGB V*) verarbeiten, sofern die **Voraussetzungen der Absätze 2 bis 4** erfüllt sind.

(2) Die Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes darf **nur**

1. im **Inland**,
2. in einem Mitgliedstaat der **Europäischen Union** oder
3. in einem diesem nach § 35 Absatz 7 des Ersten Buches gleichgestellten Staat oder, **sofern** ein **Angemessenheitsbeschluss** gemäß Artikel 45 der Verordnung (EU) 679/2016 **vorliegt**, **in einem Drittstaat** erfolgen **und sofern die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt**.

(3) Eine Verarbeitung nach Absatz 1 ist nur zulässig, wenn **zusätzlich zu den Anforderungen des Absatzes 2**

1. nach dem Stand der Technik **angemessene technische und organisatorische Maßnahmen** zur Gewährleistung der Informationssicherheit ergriffen worden sind,
2. ein **aktuelles C5-Testat** der **datenverarbeitenden Stelle** im Hinblick auf die C5-Basiskriterien für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegt und
3. die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umgesetzt sind.

Cloud Computing Anforderungskataloge

§

Bundesamt für Sicherheit in der Informationstechnik

➢**C5: Cloud Computing Compliance Criteria Catalogue**

- Kriterien zur Beurteilung der Informationssicherheit von Cloud Diensten
- Mit dem Kriterienkatalog soll den Kunden eine Hilfestellung bei der Auswahl des Cloud Provider gewährt werden
- Aufbau für eine Prüfung durch Wirschaftsprüfer gem. internationaler Prüfungsstandards geeignet
- C5-Testate können im Rahmen von Audits hilfreich sein
- Aktuell: C5:2020 → Update wohl im Dezember 2025 (“C5:2025”)

§

❑ **Beachte Landeskrankenhausgesetze**

→ **Vorrang vor § 393 SGB V!**

z.B. BayKrG, Art. 27, Absatz 6

„Im Anwendungsbereich der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO), insbesondere ***Art. 28 DSGVO (Auftragsverarbeiter)*** *und Art. 32 DSGVO (Sicherheit der Verarbeitung), sind* ***besondere Schutzmaßnahmen technischer und organisatorischer*** *Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.“*

Besonderheit: Technische & Org. Massnahmen

§

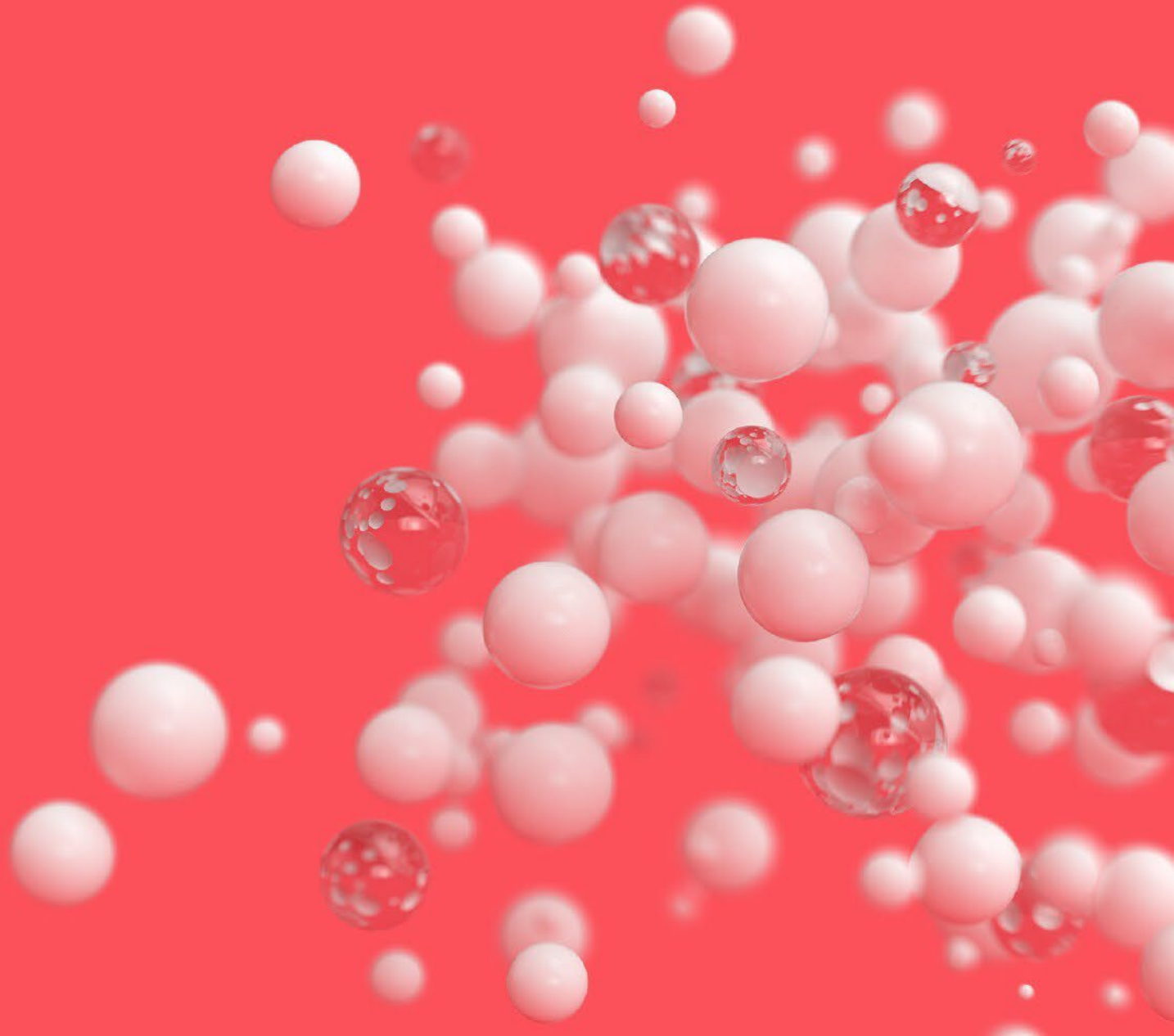
❑ **§ 22 Abs. 2 BDSG: Verarbeitung „besonderer Kategorien“ von Daten**

- „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person“ zu treffen, z.B. könnten das sein:
  - **Besondere** technische und organisatorische Maßnahmen
  - **Verschlüsselung** der Datenübermittlung
  - **Sensibilisierung** der an Verarbeitungsvorgängen Beteiligten
  - **Beschränkung des Zugangs** zu den personenbezogenen Daten bei der verantwortlichen Stelle und beim Auftragsverarbeiter

➢ **Bei Auftragsdatenverarbeitung vom Service Provider zu beachten!**

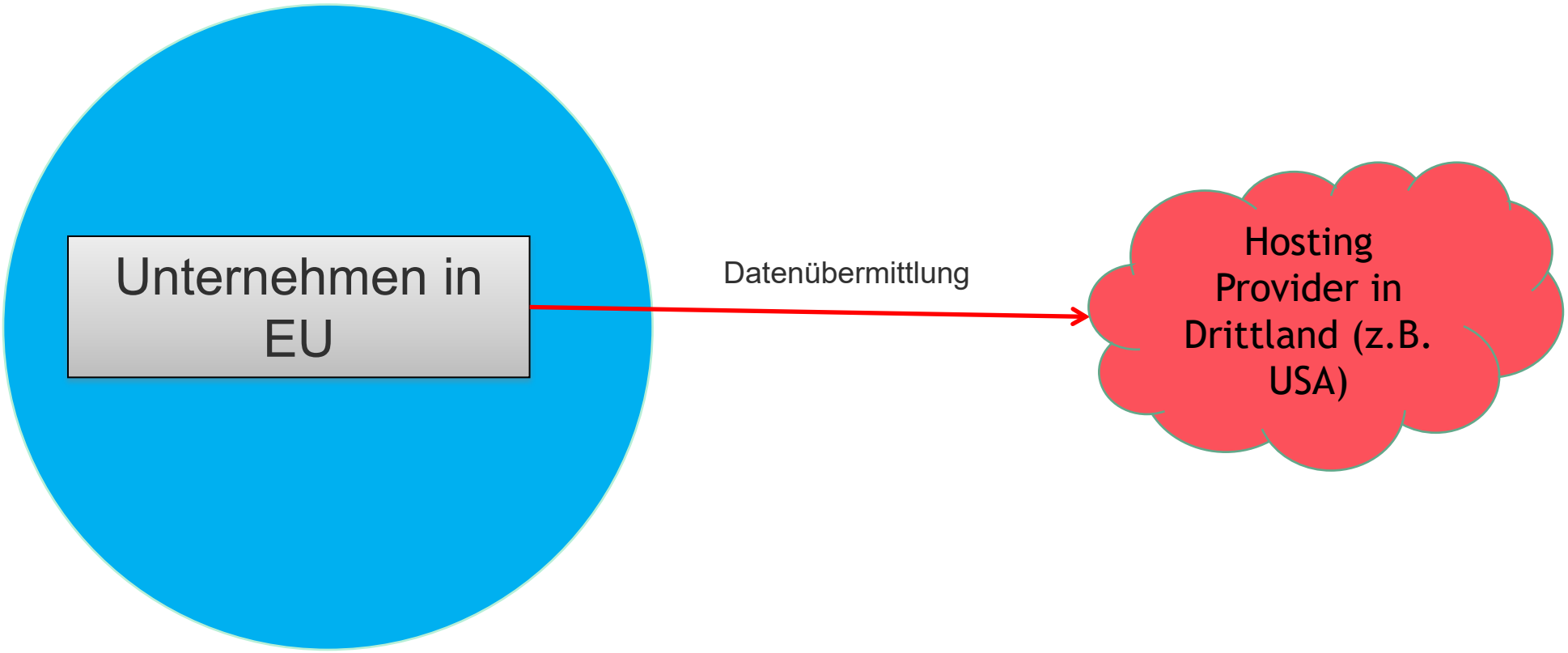
Datentransfers & Cloud Computing

Besonderheiten bei Datentransfers in Drittland

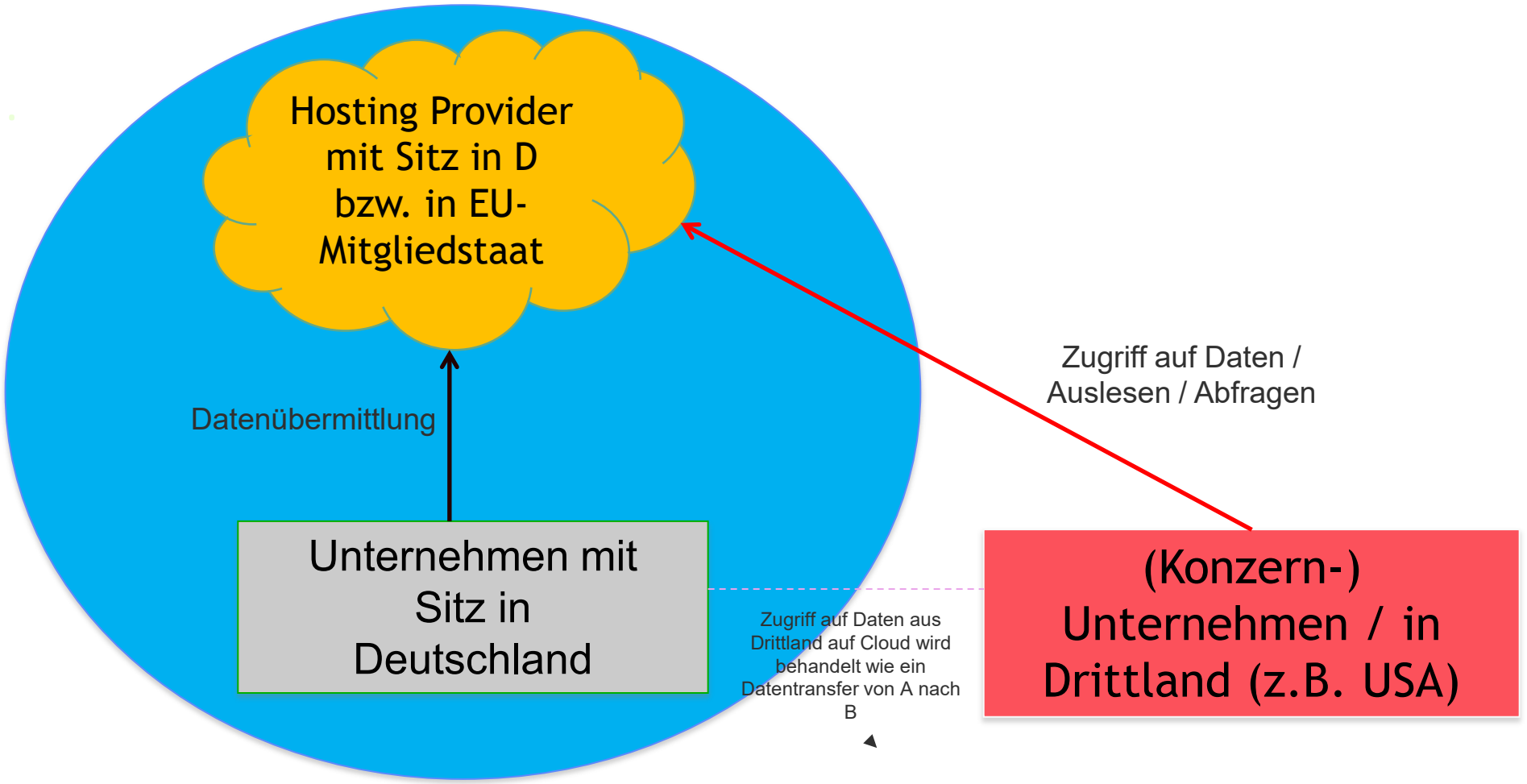


§

Datentransfer in Drittland (I)



Datentransfer in Drittland (II)



§

Zwei-Stufen Prüfung (Art. 44)

1. **Stufe:**

   Erlaubnistatbestand / Einwilligung / <u>Auftragsverarbeitung</u> (Art. 44 Abs. 1 Satz 1 u. Art.5-11)

2. **Stufe:**

   angemessenes Datenschutzniveau im Drittland?

   - **Angemessenheitsbeschluss EU-Kommission** (Art. 45)
   - **geeigneter Garantien** (Art. 46), insbesondere
     - Binding Corporate Rules (Art 46 Abs. 2 lit. b, 47)
     - EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c)
   - **Ausnahmen für best. Fälle** (Art. 49), z.B.
     - Einwilligung
     - zur Vertragsdurchführung mit Betroffenem erforderlich
     - Im öffentlichen Interesse/zur Durchsetzung von Rechtsansprüchen

§

EU-Angemessenheitsbeschlüsse

Möglichkeit der EU-Kommission verbindlich (positiv) festzustellen, ob Drittstaaten über angemessenes Datenschutzniveau verfügen

adäquates Datenschutzniveau festgestellt für:

- UK
- Israel, Japan, Kanada, Schweiz
- Andorra, Argentinien, Färöer Inseln, Guernsey, Isle of Man, Jersey, Neuseeland, Uruguay
- **USA**:
  - ~~Privacy Shield~~ → **Schrems II (EuGH 16.07.2020, C-311/18)**
  - **EU-US Data Privacy Framework (10. Juli 2023)**

<u>nicht</u> positiv festgestellt für:

- (u.a.) China, Indien, Brasilien, Russland

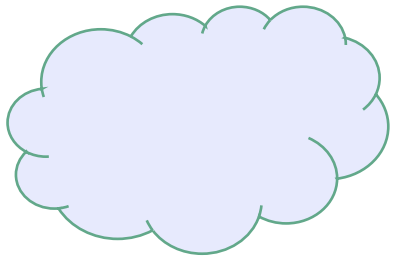
EU-Standardvertragsklauseln vom 4. Juni 2021

§

❑ **Im Licht von Schrems II: EU Kommision veröffentlicht neu SCCs**

❑ **Standardvertragsklauseln-NEU → Modularer Aufbau:**

- **Modul Eins**: Controller to Controller
- **Modul Zwei**: Controller to Processor
- **Modul Drei**: Processor to (Sub-) Processor (NEU)
- **Modul Vier**: Processor to Controller (NEU)



Schrems II – Auswirkung auf SCCs

§

❑Problem

- **Man kann sich nicht <u>per se</u> auf Standardvertragsklauseln verlassen!**
- Datenexporteure müssen sorgfältig vorab prüfen, ob der Datenempfänger in der Lage sein wird, die in den Standardvertragsklauseln dargelegten Verpflichtungen einzuhalten.
- Die nationalen Gesetze und Vorschriften des jeweiligen Drittlandes könnten sich negativ auf die Einhaltung der Standardvertragsklauseln auswirken

Wenn „Widerspruch zu nationalen Gesetzen“ vorliegt:

Standardvertragsklauseln dürfen nur mit „**geeigneten zusätzlichen Massnahmen**“ (technisch, organisatorisch, vertraglich) verwendet werden.

European Data Protection Board: Empfehlung zu „ergänzenden Massnahmen“

§

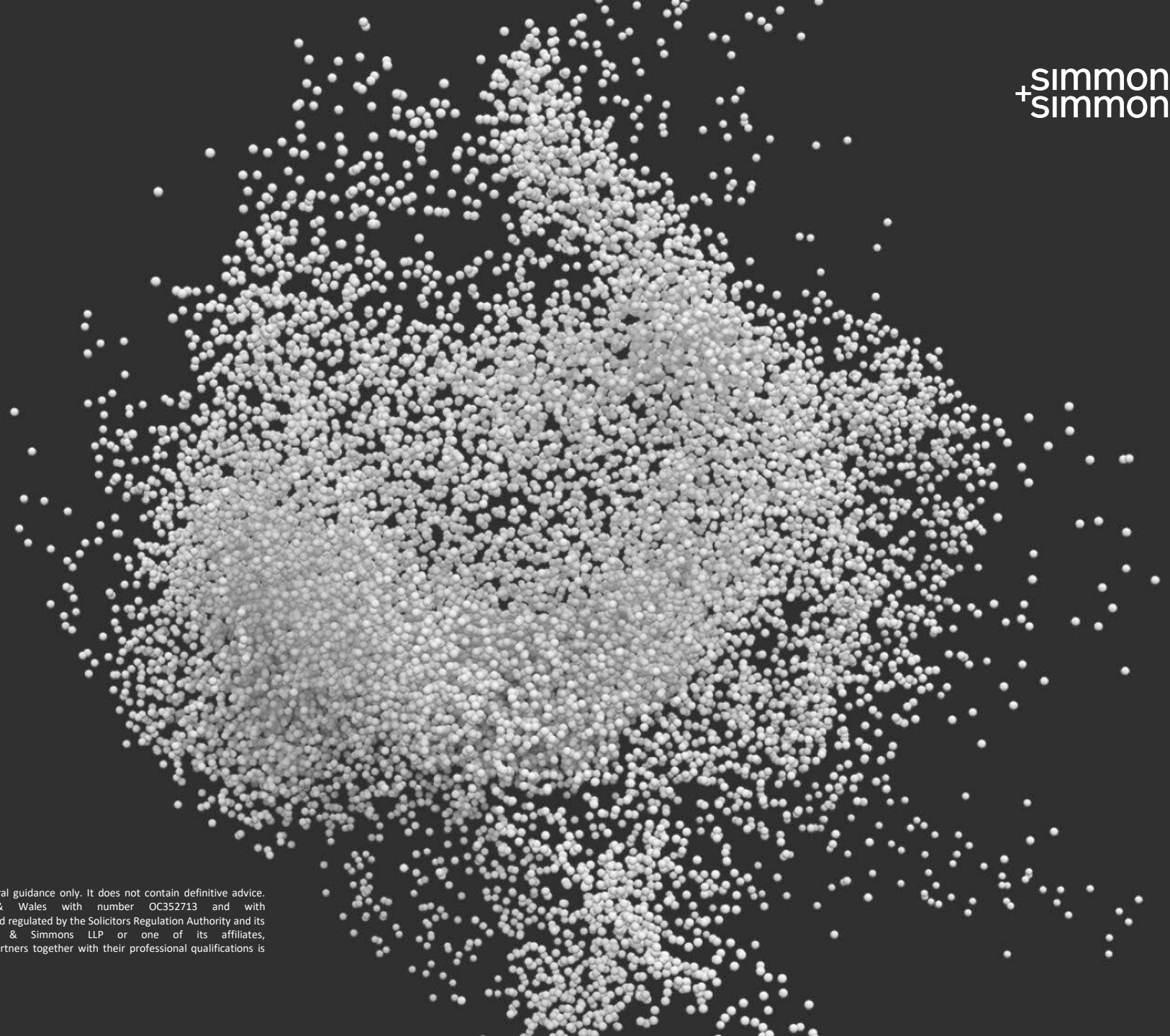
- **Data Transfer Impact Assessment - Roadmap:**
  - **Step 1:** „Know your transfers“ → Verfahrensverzeichnis!
  - **Step 2**: „Identify transfer tool you are relying on“ (z.B. AdäquanzE‘, SCCs, BCRs, Art. 49)
    - **Sofern SCCs / BCRs = Grundlage für Datentransfer:**
    - **Step 3**: Prüfung, ob im konkreten Fall „effektiv“
      - Bieten die **Gesetze des Drittlandes** den Betroffenen **effektive / durchsetzbare Rechte**?
        → **Analyse des Drittland-Rechts nötig!**
      - **Konkreten Umstände**: Datenkategorien / Speicherung im Drittland / blosser Zugriff aus Drittland etc.
    - **Step 4:** Identifiziere & implementiere geeignete ergänzende Massnahmen
      - Ziel: Abwendung pot. Gefahren für pers.bez. Daten
      - **Annex 2 der Recommendations**: Beispiele (tech / vertragl. / org.)

§

Vielen Dank für Ihre Aufmerksamkeit!

Christopher Götz, LL.M. (New York)

Partner
Rechtsanwalt
Attorney-at-law (New York)
Simmons & Simmons LLP
Tel. +49 89 20 80 77 63 – 32
Mobile: +49 151 16 24 40 50
christopher.goetz@simmons-simmons.com



simmons-simmons.com

STRICTLY PRIVATE AND CONFIDENTIAL